UNITED STATES PATENT AND TRADEMARK OFFICE

FWS

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,521	11/26/2003	Ron Ben-Natan	GRD03-01	8680

7590 05/22/2006

Barry W. Chapin, Esq.
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, MA 01581

EXAMINER	
KIM, PAUL	

ART UNIT	PAPER NUMBER
2161	

DATE MAILED: 05/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/723,521	BEN-NATAN, RON	
	Examiner	Art Unit	
	Paul Kim	2161	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☒ ~~Claim(s) *20* is/are objected to.~~

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *27 April 2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responsive to the following communication: Original Application filed on 26 November 2003.

2. Claims 1-43 are pending and present for examination. Claims 1, 20, 24, and 40-43 are independent.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description:

- Reference character 106 on line 22 of page 14.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description:

- Reference character 206 of Figure 4; and
- Reference character 219 of Figure 6.

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only

one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

5. **Claim 20** is objected to because of the following informalities: lines 10-19 of the claim read on processes of an overall limiting process. Therefore, line 16 requires the insertion of the term "and" after "security policy;". Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. **Claim 42** is rejected under 35 U.S.C. 101 because to non-statutory subject matter. The claims are directed toward "a computer data signal having program code" and are non-statutory because they do not encompass tangible subject matter and/or embodiments which fall within a statutory category.

The claims make no mention of a tangible medium wherein existing code may be processed to perform the recited steps in the claims. See State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. MPEP 2106. "The claimed invention as a whole must accomplish a practical application. That is, it must produce a 'useful, concrete and tangible result' " (emphasis added).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. **Claims 1-4, 7-9, 12, 15-27, 30-32, 35, 38-39, and 41-43** are rejected under 35 U.S.C. 102(e) as being anticipated by Cook et al (U.S. Patent No. 6,820,082, hereinafter referred to as COOK), filed on 3 April 2000, and issued on 16 November 2004.

10. **As per independent claims 1 and 41-43**, COOK teaches:

A method (and computer program product, computer data signal, or data security filter device) of security enforcement for a persistent data repository comprising:

intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items {See COOK, col. 5, lines 42-67, wherein this reads over in part "access manager receives queries from the user interface, processes the queries as described below, and sends the modified queries or query to the data access manager"};

determining if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access {See COOK, col. 2, lines 54-65, wherein this reads over "[t]he reul engine includes a plurality of security rules and is operable to evaluate the request against the plurality of rules . . . [which] are based on a relation between the user and the data"}; and

limiting, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction {See COOK, col. 8, lines 46-61, wherein this reads over in part "[t]he access manager will combine this query with the security rule defined above to form the following modified query" and "returned data may also be filtered by applying additional security rules to the data"}.

11. **As per dependent claims 2 and 25**, COOK teaches:

The method of claim 1 wherein the security policy has rules {See COOK, col. 9, lines 2-3, wherein this reads over "[s]ecurity policies can be changed by simply modifying the rules within the rule engine"}, each of the rules including an object, a selection criteria and an action, the action indicative of restricted data items {See COOK, col. 2, lines 61-65, wherein this reads over "a plurality of security rules . . . to determine if the user has authority to perform requested action with respect to the data"}.

12. **As per dependent claims 3 and 26**, COOK teaches:

The method of claim 1 wherein the data indications are references to data items in the data repository {See COOK, col. 5, lines 58-61, wherein this reads over "data obtained from the database to control access to the data by the user"} and limiting further includes qualifying the references to generate a modified request indicative of unrestricted data items, such that successive retrieval operations employing the qualified references do not retrieve restricted data items {See COOK, col. 7, lines 61-64, wherein this reads over "security constraints may be applied to the incoming query and processed in the access manager to form a modified query which is sent to the data manager"}.

13. **As per dependent claims 4 and 27**, COOK teaches:

The method of claim 3 wherein the data access transaction is a data access statement operative to request data and limiting further comprises:

identifying at least one rule, according to the security policy, corresponding to the data access statement, the identified rule restricting access to at least one of the data items indicated by the data access statement {See COOK, Table 1; col. 7, lines 42, wherein this reads over "object-level security applies to an entire row of data"; and col. 8, lines 34-35, wherein this reads over "[t]he rule engine includes the following user defined security rule for Table 2"}, and

concatenating selection qualifiers to the data access statement corresponding to the identified rule, {See COOK, col. 8, lines 45-53, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query for a user"} the selection qualifiers operable to omit the restricted data items from the qualified references of the data access statement {See COOK, col. 8, lines 57-59, wherein this reads over "the database which will return the sales data from rows 1 and 3 of Table 2"}.

14. **As per dependent claims 7, 21, and 30**, COOK teaches:

The method of claim 2 wherein the actions are selectively indicative of modifications, the modifications further comprising attributes, operators, and operands, the limiting further comprising

identifying data items corresponding to the attributes, each of the attributes associated with an operator and an operand {See COOK, col. 8, lines 51-53};

applying an operator specified for the data item to the operand specified for the data item {See COOK, col. 8, lines 51-53}; and

determining, as a result of applying the operator, whether to eliminate the identified data item {See COOK, col. 8, lines 51-53}.

15. **As per dependent claims 8 and 31,** COOK teaches:

The method of claim 1 wherein the nonintrusive manner is undetectable to the user application and undetectable to the data repository {See COOK, Figure 1}.

16. **As per dependent claims 9 and 32**, COOK teaches:

The method of claim 1 wherein intercepting the data access transaction further comprises:

establishing a proxy to the data repository on behalf of the user {See COOK, Figure 1, Element 70};

receiving the data access transaction as a row set under the proxy {See COOK, col. 5, lines 51-54, wherein this reads over "access manager receives queries from the user interface, process the queries as described below"}; and wherein limiting includes:

regenerating the resulting data access transaction as a reduced row set having a subset of the rows from the proxy row set {See COOK, col. 7, lines 61-63, wherein this reads over "security constraints may be applied to the incoming query and processed in the access manager to form a modified query which is sent to the data manager"}; and

transmitting the reduced row set to the user on behalf of the proxy {See COOK, Figure 6, step 122; and col. 11, lines 10-12, wherein this reads over "[t]he page generator outputs a page formatted using visible data from the database"}.

17. **As per dependent claims 12 and 35**, COOK, in combination with FISHER, discloses:

The method of claim 4 wherein intercepting the data access statement includes

receiving an SQL query {See COOK, col. 8, lines 57-59, wherein this reads over "[t]he data manager will format this query as an SQL query and submit it to the database"} and

limiting includes appending conditional selection statements to the SQL query, the conditional selection statements computed from the security policy, to generate the resulting data access transaction {See COOK, col. 8, liens 45-50, wherein this reads over "[t]he access manager will combine this query with the security rule defined above"}.

18. **As per dependent claim 15**, COOK teaches:

The method of claim 1 wherein the nonintrusive manner is such that the intercepting and limiting occurs undetectable to both the source and the destination of the data access transaction {See COOK, Figure 1}.

19. **As per dependent claim 16**, COOK teaches:

The method of claim 1 wherein intercepting further comprises:

establishing an identification exchange intended for interception and operable to transmit an identification token indicative of an application user {See COOK, Tables 3 and 4; col. 4, lines 60-61, wherein this reads over "the user . . . is identifiable by a user ID"; and col. 8, lines 34-53}; and

parsing, as part of the intercepting, the identification exchange to extract the identification token {See COOK, Tables 3 and 4, and col. 8, lines 34-53}, wherein the identification exchange is benign to the data repository {See COOK, col. 10, line 66 – col. 11, line 13, wherein this reads over "further filter the data returned from the database by removing information that is not available to the user"}.

20. **As per dependent claims 17 and 38**, COOK teaches:

The method of claim 1 wherein intercepting occurs in a data path between a source of the data access transaction and a destination of the resulting data access transaction, and limiting occurs in a component separate from the source and destination {See COOK, Figure 1}.

21. **As per dependent claims 18 and 39**, COOK teaches:

The method of claim 17 wherein the component separate from the source and destination is a separate network device than the components corresponding to the source and destination {See COOK, Figure 1}.

22. **As per dependent claim 19,** COOK teaches:

The method of claim 1 wherein the restricted data items are eliminated from the resulting data access transaction {See COOK, Figure 1}.

23. **As per independent claim 20**, COOK teaches:

A method for nonintrusive implementation of data level security enforcement comprising:

defining a security policy between an application and a data repository the security policy having rules indicative of restricted data items {See COOK, col. 9, lines 2-3, wherein this reads over "[s]ecurity policies can be changed by simply modifying the rules within the rule engine"}, the rules associated with attributes and conditions {See COOK, col. 8, lines 51-53};

identifying an entry point between the data repository and the application {See COOK, Figure 1, Element 70};

deploying a security filter at the entry point, the security filter operable to receive data manipulation messages between the application and the data repository {See COOK, Figure 1, Element 70};

the security filter further operable to limit data exposure by the data repository by selectively modifying the data manipulation messages into conformance with the security policy {See COOK, Table 1; col. 7, lines 42, wherein this reads over "object-level security applies to an entire row of data"; and col. 8, lines 34-35, wherein this reads over "[t]he rule engine includes the following user defined security rule for Table 2"}, the limiting further comprising:

sniffing the entry point to determine data manipulation messages {See COOK, col. 8, lines 51-53};

intercepting the sniffed data manipulation messages in a nondestructive manner {See COOK, col. 5, lines 42-67, wherein this reads over in part "access manager receives queries from the user interface, processes the queries as described below, and sends the modified queries or query to the data access manager"};

comparing the sniffed messages to the rules in the security policy to determine if the sniffed data manipulation message includes restricted data items

{See COOK, col. 2, lines 54-65, wherein this reads over "[t]he reul engine includes a plurality of security rules and is operable to evaluate the request against the plurality of rules . . . [which] are based on a relation between the user and the data"};

determining if the sniffed messages match at least one of the rules of the security policy {See COOK, col. 2, lines 61-65, wherein this reads over "a plurality of security rules . . . to determine if the user has authority to perform requested action with respect to the data"};

selectively modifying, if the determining indicates a match between the rules and the data manipulating message, the data manipulation message to remove the matching restricted data item {See COOK, col. 8, lines 46-61, wherein this reads over in part "[t]he access manager will combine this query with the security rule defined above to form the following modified query" and "returned data may also be filtered by applying additional security rules to the data"}.

24. **As per dependent claim 22**, COOK teaches:

The method of claim 20 wherein modifying further comprises:

reconstructing a request query corresponding to a query syntax {See COOK, col. 8, lines 45-53, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query for a user"}; and

adding limiters to the request query corresponding to the matching rules of the security policy {See COOK, col. 8, lines 45-53, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query for a user"}, the adding performed in a nondestructive manner such that the modification is undetectable to the data repository {See COOK, Figure 1}.

25. **As per dependent claim 23**, COOK teaches:

The method of claim 20 wherein modifying further comprises:

identifying a data retrieval response encapsulated in a layered protocol on the data manipulation message {See COOK, col. 5, lines 42-67, wherein this reads over in part "access manager receives queries from the user interface, processes the queries as described below, and sends the modified queries or query to the data access manager"}; and

reconstructing the data retrieval response by deleting restricted data items from the data retrieval response, the reconstructing performed in a nondestructive manner undetectable to the application and conforming to the encapsulating layered protocol {See COOK, col. 8, lines 1-2, wherein this reads over "the remaining security constraints applied to the obtained data"}.

26. **As per independent claim 24**, COOK teaches:

A data security filter device for security enforcement for a persistent data repository comprising:

an interceptor in the security filter operable to intercept, in a nonintrusive manner {See COOK, Figure 1},

a data access transaction between a user application and a data repository having data items {See COOK, col. 5, lines 42-67, wherein this reads over in part "access manager receives queries from the user interface, processes the queries as described below, and sends the modified queries or query to the data access manager"};

a security policy table responsive to the interceptor to determine if the intercepted data access transaction corresponds to the security policy table, the security policy table indicative of restricted data items in the data repository to which the user application is prohibited access {See COOK, col. 2, lines 54-65, wherein this reads over "[t]he reul engine includes a plurality of security rules and is operable to evaluate the request against the plurality of rules . . . [which] are based on a relation between the user and the data"}; and

a limiter operable to limit, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy table, are modified in a resulting data access transaction {See COOK, col. 8, lines 46-61, wherein this reads over in part "[t]he access manager will combine this query with the security rule defined above to form the following modified query" and "returned data may also be filtered by applying additional security rules to the data"}.

Claim Rejections - 35 USC § 103

27. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

28. **Claims 5-6, 14, 28-29, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over COOK, in view of Fisher et al (U.S. Patent No. 6,085,191, hereinafter referred to as FISHER), filed on 25 March 1998, and issued on 4 July 2000.

COOK teaches the limitations of claims 1-4, 7-9, 12, 15-19, 24-27, 30-32, 35, 38-39, and 41-43 for the reasons stated above.

COOK differs from the claimed invention in that COOK fails to specifically disclose a method wherein identified rows are eliminated from the data access transaction (claims 5-6 and 28-29).

COOK differs from the claimed invention in that COOK fails to specifically disclose a method

29. **As per dependent claims 5 and 28**, COOK, in combination with FISHER, discloses:

The method of claim 1 wherein the data indications are rows of data retrieved from the data repository, and limiting further comprises:

identifying rows having restricted data items {See FISHER, col. 3, lines 29-35, wherein this reads over "[e]ach view defines a subset of rows in the database tables that are accessible when using this view"}, and

eliminating the identified rows from the data access transaction {See FISHER, col. 19, lines 39-49, wherein this reads over "[v]iews can also be used to limit the columns and rows of database tables that are accessible to users"} such that the resulting data access transaction is a modified query response including rows without restricted data items {See COOK, col. 8, lines 45-50, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query"}.

The combination of the inventions disclosed in COOK and FISHER would disclose a method wherein limiting access to and eliminating rows of data from the data access transaction would comprise the application applying a view, which defines a subset of rows in the database tables that are accessible, and applying rules of a security policy to the response to further limit access to the identified rows. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by COOK and FISHER.

One of ordinary skill in the art would have been motivated to do this modification in order to limit access to identified rows.

30. **As per dependent claims 6 and 29**, COOK, in combination with FISHER, discloses:

The method of claim 5 wherein the data access transaction is a data query response including a row set and limiting further comprises:

comparing each of the rows in the row set to the rules of the security policy {See COOK, col. 8, lines 57-59, wherein this reads over "data manager will format this query as an SQL query and submit it to the database which will return the sales data from rows 1 and 3 of Table 2"}; and

selectively eliminating rows in the row set including the restricted data items, based on the comparing, to generate a modified query response including a filtered row set {See COOK, col. 8, lines 45-50, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query"}.

The combination of the inventions disclosed in COOK and FISHER would disclose a method wherein the row set of the data query response is compared to and filtered by the rules of the security policy. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by COOK and FISHER.

One of ordinary skill in the art would have been motivated to do this modification in order to limit access to identified rows.

31. **As per dependent claims 14 and 37**, COOK, in combination with FISHER, discloses:

The method of claim 6 wherein intercepting the data query response further comprises:

intercepting the data query response from the data repository as the data access transaction {See FISHER, col. 28, lines 53-64, wherein this reads over "Step 1612 . . . which intercepts a user access request to access management information stored in managed objects stored in a desired table in the database"},

the data query response encapsulated as a row set having rows from a relational database query {See COOK, col. 8, lines 57-59, wherein this reads over "return the sales data from rows 1 and 3"} and further wherein limiting includes

discarding rows in the row set having restricted data items {See COOK, col. 8, lines 45-50, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query"} and

transmitting the remaining rows to the user as the resulting data access transaction {See COOK, Figure 6, step 122; and col. 11, lines 10-12, wherein this reads over "[t]he page generator outputs a page formatted using visible data from the database"}.

The combination of the inventions disclosed in COOK and FISHER would disclose a method wherein the data query response from the data repository is intercepted and rows are discarded accordingly. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by COOK and FISHER.

One of ordinary skill in the art would have been motivated to do this modification in so that restricted data items may be eliminated and the remaining rows transmitted to the user.

32. **Claims 10-11 and 33-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over COOK, in view of Bechtolsheim et al (U.S. Patent No. 7,043,541, hereinafter referred to as BECHTOLSHEIM), filed on 21 September 2000, and issued on 9 May 2006.

COOK teaches the limitations of claims 1-4, 7-9, 12, 15-19, 24-27, 30-32, 35, 38-39, and 41-43 for the reasons stated above.

COOK differs from the claimed invention in that COOK fails to disclose a method for padding packets such that restricted data items may be eliminated (claims 10 and 33).

COOK differs from the claimed invention in that COOK fails to disclose a method for preserving the encapsulating layered protocol (claims 11 and 34).

33. **As per dependent claims 10 and 33**, COOK, in combination with BECHTOLSHEM, discloses:

> The method of claim 1 wherein limiting the data access transaction further includes receiving a set of packets, the packets encapsulating the data access transaction according to layered protocols;
>
> > interrogating and modifying the packets in a nondestructive manner with respect to the layered protocols {See COOK, col. 8, liens 45-50, wherein this reads over "[t]he access manager will combine this query with the security rule defined above"}; and
> >
> > padding the packets for accommodating elimination of the restricted data items to generate the resulting data access transaction {See BECHTOLSHEM, col. 8, lines 47-48, wherein this reads over "[s]hort packets are padded to 64 bytes"}.

The combination of the inventions disclosed in COOK and BECHTOLSHEM would disclose a method wherein packets are modified in a nondestructive manner by padding the packets to accommodate the addition of restrictive limiting language to the query. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by COOK and BECHTOLSHEM.

One of ordinary skill in the art would have been motivated to do this modification so that the changes in the query may be nondetectable yet still be modified to include the restrictive language of the security policy.

34. **As per dependent claims 11 and 34**, COOK, in combination with BECHTOLSHEM, discloses:

> The method of claim 10 wherein generating the resulting data access transaction preserves the encapsulating layered protocol associating the packets without employing a proxy for regenerating the sequence of packets {See COOK, col. 8, lines 57-59, wherein this reads over "return the sales data from rows 1 and 3"}.

The combination of the inventions disclosed in COOK and BECHTOLSHEM would disclose a method wherein the encapsulating layered protocol is preserved without employing a proxy. Therefore, it

would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by COOK and BECHTOLSHEM.

One of ordinary skill in the art would have been motivated to do this modification so that a proxy need not be necessarily employed in generating a resulting data access transaction.

35. **Claims 13, 36, and 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over COOK, in view of Slutz (U.S. Patent No. 6,581,052, hereinafter referred to as SLUTZ), filed on 2 October 2000, and issued on 17 June 2003.

COOK teaches the limitations of claims 1-4, 7-9, 12, 15-19, 24-27, 30-32, 35, 38-39, and 41-43 for the reasons stated above.

COOK differs from the claimed invention in that COOK fails to disclose a method for building a parse tree (claims 13 and 36).

36. **As per dependent claims 13 and 36**, COOK, in combination with SLUTZ, discloses:

The method of claim 12 further comprising:

building a parse tree corresponding to the SQL query {See SLUTZ, Figures 6 and 8};

adding nodes in the parse tree corresponding to the appended conditional selection statements {See SLUTZ, col. 11, lines 3-14, wherein this reads over "updates the statement according to the choices made . . . [wherein] a choice at each current node adds a term to the statement's parse tree"}; and

reprocessing the parse tree to generate the resulting data access transaction {See SLUTZ, Figure 6; and col. 9, lines 26-29, wherein this reads over "outputs a representation of the statement to program as the statement is generated"}.

The combination of the inventions disclosed in COOK and SLUTZ would disclose a method for building a parse tree corresponding to the SQL query and adding nodes corresponding to the appended conditional selection statements. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by COOK and SLUTZ.

One of ordinary skill in the art would have been motivated to do this modification so that the appended conditional selection statements may be added as nodes to the parse tree.

37. **As per independent claim 40**, COOK, in combination with SLUTZ, discloses:

A method for nonintrusive implementation of data level security enforcement comprising

defining a security policy having rules {See COOK, col. 9, lines 2-3, wherein this reads over "[s]ecurity policies can be changed by simply modifying the rules within the rule engine"}, the rules further specifying attributes and conditions {See COOK, col. 8, lines 51-53};

intercepting a data retrieval request {See COOK, col. 5, lines 42-67, wherein this reads over in part "access manager receives queries from the user interface, processes the queries as described below, and sends the modified queries or query to the data access manager"};

comparing the data retrieval request to the security policy {See COOK, col. 2, lines 54-65, wherein this reads over "[t]he reul engine includes a plurality of security rules and is operable to evaluate the request against the plurality of rules . . . [which] are based on a relation between the user and the data"};

determining if the data retrieval request corresponds to at least one of the rules of the security policy {See COOK, col. 2, lines 54-65, wherein this reads over "[t]he reul engine includes a plurality of security rules and is operable to evaluate the request against the plurality of rules . . . [which] are based on a relation between the user and the data"};

identifying, via a parse tree {See SLUTZ, Figures 6 and 8}, selectivity operators indicative of the data to be retrieved {See SLUTZ, Figures 6 and 8; COOK, col. 8, lines 51-53};

modifying the parse tree according to the corresponding rule to generate a modified data retrieval request {See SLUTZ, col. 11, lines 3-14, wherein this reads over "updates the statement according to the choices made . . . [wherein] a choice at each current node adds a term to the statement's parse tree"}; and

forwarding the modified data retrieval request to the data repository for subsequent retrieval and transport to the requesting user {See COOK, Figure 1}.

The combination of the inventions disclosed in COOK and SLUTZ would disclose a method for building a parse tree corresponding to the SQL query and adding nodes corresponding to the appended conditional selection statements. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by COOK and SLUTZ.

One of ordinary skill in the art would have been motivated to do this modification so that the appended conditional selection statements may be added as nodes to the parse tree, and consequently generating a retrieval request from the aforementioned parse tree, to be forward to the data repository for subsequent retrieval and transport of data items to the requesting user.

Conclusion

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Kim whose telephone number is (571) 272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Gaffin can be reached on (571) 272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Paul Kim
Patent Examiner, Art Unit 2161
Technology Center 2100

SAM RIMELL
PRIMARY EXAMINER